IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Proudler, Graeme John	Examiner:	Moran, Randal
Serial No.	10/688,397	Art Unit:	2135
Filed:	10/16/2003	Our Ref:	621375 200309650
For:	"Method and Apparatus for Managing a Hierarchy of Nodes"	Date:	February 4, 2008
		Re:	***Brief on Appeal***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated September 5, 2007, for the above identified patent application. A Notice of Appeal was filed on December 4, 2007 with a certificate of mailing attached. Appellants submit that this Appeal Brief is being timely filed on February 4, 2008. Please charge the Appeal Brief fee of $510.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A.

(hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 35-42, 44 and 46-49 are present in the application. Claims 1-34, 43 and 45 have been canceled without prejudice. Claims 35-42, 44 and 46-49 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

No amendments have been proffered in response to the Final Rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to an apparatus for managing a hierarchy of keys used by a trusted computing platform for the protection of sensitive data. A trusted computing platform has a tree-structured key hierarchy the non-leaf nodes of which each comprise, in encrypted form, a key used to encrypt the or each of its child nodes. The leaf nodes need not be keys. Such a tree is used to provide "protected storage" for a trusted platform according to TCG specifications (TCG is the Trusted Computing Group which is the successor to the TCPA group mentioned in the specification). The root key of the key hierarchy is called the "storage root key" or "SRK" in the present application and is held in decrypted

form in secure storage forming part of a "trusted platform module" or TPM. The present invention concerns the ability of replacing the storage root key (SRK) with a key lower in the hierarchy (such a key is called a dynamic root key or DRK in the specification); in this state, only those hierarchy nodes below the dynamic root key currently replacing the storage root key can be accessed. Those parts of the hierarchy that could only be reached by ascent from the original storage root node, and not via the dynamic root key, become inaccessible. (Figures 1 and 3, p. 4, l. 13 to p. 5, l. 2, and p. 6, l. 30 to p. 12, l. 2).

Claim 35 is directed to a computing platform comprising:

a secure key-handling unit (10) arranged to store a storage root key (11) that forms the root node of a tree-structured node hierarchy the non-leaf nodes (K1-1, K1-2, K1-3 etc.) of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes (K2-1, K2-2, etc.), and

insecure storage (22) for storing the hierarchy nodes other than the root node;

the key-handling unit comprising:

a memory (10) for storing a current decryption-root key;

a decrypted-access arrangement (10) arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key; and

a current-decryption-root setting arrangement (10) for storing in said memory, in decrypted form, the key (16) of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 35-42, 22 and 46-49 are patentable under 35 U.S.C. 103(a) in view of Challenger (US2002/0059286) alone and when considered with Ishiguro (US 5796839)?

ARGUMENT

Issue 1: Whether Claims 35-42, 44 and 46-49 are patentable under 35 U.S.C. 103(a) in view of Challener (US2002/0059286) alone and when considered with Ishiguro (US 5796839)?

In the Final Office Action of September 5, 2007, the Examiner rejects Claims 35-42, 44 and 46-49 under 35 U.S.C. §103(a), as being obvious over Challener. See page 2 of the official action. However when discussing the rejection, the Examiner mentions both Challener and a document which the Examiner merely identifies as Ishiguro. See page 3 of the official action.

A rejection based on Challenger alone must fail since the Examiner admits that Challenger does not meet all of the limitations of claim 35 (and hence also does not meet all of the limitations of the claims which depend therefrom). The Examiner's admission can be found on page 3 of the official action.

The Examiner asserts that Ishiguro allegedly teaches that which Challener does not teach. See page 3 of the official action. The first issue which must be considered is what document is the Examiner referring to when he simply mentions "Ishiguro" on page 3 of the official action. There are two "Ishiguro" references listed on the "Notice of

References Cited" which accompanies the official action. The Applicant believes that the reference to "Ishiguro" on page 3 of the official action is meant to refer to US Patent 5796839 to Ishigure rather than to US Publication 2006/0159272 to Ishiguro since the Examiner states on page 6 of the official action that US Publication 2006/0159272 and others are not relied upon by the Examiner.

Claim 35 and the Challener Reference - Does Challener teach that which the Examiner Asserts in the Final Rejection?

Challener relates to the same type of protected storage hierarchy as the present application and therefore has a storage root key heading a node hierarchy in which the non-leaf nodes each comprise a key used to encrypt the or each of its child nodes This actually is not well described in Challener though a skilled person would fully understand this and paragraph [0021] does provide a brief description.

Challener discloses the first part of applicant's claim 35:

> "A computing platform comprising:
> a secure key-handling unit arranged to store a storage root key that forms the root node of a tree-structured node hierarchy the non-leaf nodes of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes, and
> insecure storage for storing the hierarchy nodes other than the root node;"

The rest of claim 35 details the key-handling unit:

> "the key-handling unit comprising:
> a memory for storing a current decryption-root key;
> a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key; and
> a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed."

These features provide the ability to limit the decryptable nodes to those depending from a selected non-leaf node, the key associated with this node being decrypted and stored in the memory as the "current decryption root key"

The Examiner argues at the top of page 3 of the Final Official Action that Challener teaches "the decrypted-access arrangement" (but not the current-decryption-root setting arrangement). However, Challener does not have any arrangement for restricting "decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key". This is because the only "current decryption-root key" disclosed in Challener is the storage root key itself and all the hierarchy nodes are decryptable by a chain of decryption rooted in the storage root key – therefore there is no concept of less than the whole hierarchy being decryptable in Challener and therefore no concept of an arrangement restricting decrypted access to a subset of the nodes of the hierarchy.

The Examiner's assertions regarding Challener imply an assumption that the recited storage root key and the recited current decryption-root key are the same. But that is incorrect assumption in view of the final limitation which clearly indicates that not only are they different (because one is at the root of the hierarchy and the other is a selected non-leaf node of the hierarchy), but that the current decryption-root key is changeable.

The Examiner reads more into Challener than Challener teaches. As such, Challener does not teach each and every limitation subscribed to it by the Examiner in the Final Rejection.

The Ishiguro Reference (US 5,706,839)

Ishiguro teaches a method and apparatus for encrypting software or data, particularly data and software distributed on DVDs having a series of versions thereof.

Ishiguro discloses a linear hierarchy of keys in which each key is derived from its parent by a one-way function, starting with a master key (see Figure 2, where the master key is referenced K0). An important point to note about this hierarchy is that it does not actually exist in its entirety at any time – generally, there will only exist at any one time in any apparatus:

> a master key (or alternatively the highest available key in the logical hierarchy); a key lower in the hierarchy that has been generated from the master key using a one way function. See c. 3, l. 30-39 and c. 4, l. 25-31.

In fact, this is the attraction of the arrangement proposed in Ishiguro – that key management in user apparatus (decoding apparatus) is made simple as only one key need be stored, all other keys below it in the hierarchy being derivable from that key. For example, if a user has, for example, the encryption key of a version 3 of software or data, then the user can decode the earlier versions, 1 and 2, of that software or data, but not a later version, such as a version 4. This is not well described in Ishiguro, but see the paragraph bridging c. 4 and 5 of Ishiguro.

The encrypting method and apparatus of Ishiguro are described at c. 5, l. 14-60 with reference to Fig. 3 to 5. In fact, the description is very sparse and simply says that a "work key" is selected from the Figure 2 hierarchy – there is no description of the selection process and so no reason to think it is done by first generating and storing all hierarchy keys. It is much more likely that, starting from the master key, successive generations of keys are generated in turn until a desired generation is reached (this is what is done in the decoding apparatus - see below). Once selected, the work key is then used to encrypt reference data (called a "magic number") and the plain text to be

encrypted. The encrypted plain text (the 'cipher text') is then recorded onto a DVD along with the encrypted magic number.

Decoding (decrypting) of the DVD is primarily described at c. 5, l. 61 to c. 6, l. 67 with reference to Figures 6 to 8. Beginning with the master key (or, as mentioned at col. 7, line 22, the latest available encryption key), successive generations of keys are generated in turn and each used to encrypt the magic number until the encrypted magic number so produced matches that on the DVD; at this point the key concerned is set as the "work key" and used to decrypt the cipher text on the DVD.

Claim 35 and the Ishiguro Reference - Does Ishiguro teach that which the Examiner Asserts in the Final Rejection?

The examiner argues in the second half of page 3 of the Action that Ishiguro discloses the following claim 35 elements:

> the memory for storing a current decryption-root key; and
> the current-decryption-root setting arrangement.

Since Ishiguro discloses, in connection with the embodiment of Figure 9, the possibility of setting any of the encryption keys into decoding apparatus to serve as the starting key for generating descendant keys of the hierarchy, we agree that Ishiguro discloses the current-decryption-root setting arrangement. Ishiguro must also implicitly have a memory for storing the key acting as the current decryption root key.

However, applicant does not agree with the Examiner's analysis set out on page 3 as what he appears to be saying is that the "work key" of Ishiguro (the key stored in register 13 of the Figure 6 decoding apparatus) equates to the "current decryption root key" of claim 35. From Figure 7 and the passage running from col. 6, line 20 to col. 7, line 7 of Ishiguro, it is clear that the work key stored in memory 13 is only used to

decrypt the cipher text from the DVD (step S13). The work key is not used as the root key enabling decryption of dependent nodes of the hierarchy.

The key of Ishiguro that most closely corresponds to the "current decryption root key" of claim 35 is the key to which 'k' is set in step S21 of Figure 8 (this being the algorithm for generating the work key). In the embodiment described with respect to Figures 6 to 8, 'k' is set in step S21 to the master key. However, as already noted, Ishiguro also discloses in relation to the Figure 9 embodiment, the possibility of initially setting 'k' to the latest available encryption key ki (see col.7, lines 13 – 38 and step S31 of Figure 9).

In Ishiguro, the initial value of k (set to the master key in step S21, or to the latest encryption key ki in S31) determines what other nodes of the hierarchy are accessible and therefor most closely corresponds to the "current decryption root key" of claim 35.

An important point to note is that: Ishiguru has no concept of an arrangement for restricting access to only some of the hierarchy nodes because Ishiguru always starts with the available key that is highest up the hierarchy. Nodes of the hierarchy that are higher up than this starting key are de facto inaccessible without any need to provide an arrangement to restrict access.

So applicant believes that the Examiner reads more into Ishiguro than Ishiguro teaches.

Considering Challener & Ishiguro Together

So, assuming for the moment that it would be obvious to combine the teachings of Challener and Ishiguro as the Examiner has done in the Final Rejection, the suggested combination still does not meet the following limitation of claim 35:

> "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key;"

In both Challener and Ishiguro, decryptable access is always rooted as high up the hierarchy as possible.

In contrast, in the claim 35 apparatus, although the storage root key is available in the key-handling unit, access to the nodes of the hierarchy is restricted to the nodes dependent from the node associated with the current decryption root key. Thus the decrypted access restriction provided by the "decrypted-access arrangement" is a important part of the claim 35 apparatus but is not something that is either needed or disclosed by Challener or Ishiguro.

Since neither Challener nor Ishiguro discloses the "decrypted-access arrangement" of claim 35, it is not reasonable to argue that combining Ishiguro and Challener will result in such an arrangement being present.

In the response dated June 5, 2007, the applicant asserted the limitation quoted above was "fairly standard". That is a mis-statement and the applicant hereby withdraws it.

The Examiner has not provided a reasonable rationale for combining the teachings of Challener & Ishiguro

Of course, 35 U.S.C. § 103 "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The Court stated that obvious analysis "should be made explicit." Id. at 1740-41, citing *In re Kahn*, 441 F.3d 977,988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must

be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

The Examiner asserts in the Final Official Action that a person of ordinary skill would be motivated to modify the teachings of Challener by the teachings of Ishiguro "to provide a decoding apparatus in which encryption keys can be managed with ease" the Examiner citing c2, l. 10-11 of Ishiguro. See the first paragraph on page 4 of the Final Rejection.

This is a mere conclusory statement. The Examiner has provided no articulated reasoning with some rational underpinning to support his legal conclusion of obviousness. The rejection under 35 USC 103(a) is improper and should be overturned.

Indeed, there would seem to be no reason to combine Challener and Ishiguro. Ishiguro has come up with an easier way of managing the encryption of DVDs so that the owner of a later version of a DVD title can decode an earlier version of the same DVD title. What possibly applicability does Ishiguro's software/data distribution scheme have to Challener's trusted computing platform which Challener equips with two storage trees in order to speed up file access? Moreover, the required security properties of the Challener TPM make it highly undesirable that the keys of its key hierarchy are cryptographically related to each other as in Ishiguro. So the very feature (ease of management of keys in the context of DVD distribution) to which the Examiner points, which uses the one way function discussed above and results the keys being cryptographically related to each other is something which would be undesirable in the system taught by Challener. Furthermore, in the embodiments of Ishiguro where the master key is available, there is no suggestion that it should be replaced by another key

- therefore, since in Challener the storage root key is always available, Ishiguro has nothing useful to offer Challener.

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable over the cited art. Therefore, reversal of all rejections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being transmitted electronically to the United States Patent and Trademark Office on

February 4, 2008
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

February 4, 2008
(Date)

Respectfully submitted,

/Richard P. Berg 28,145/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Enclosures:
Claims Appendix;
Evidence Appendix;
Related Proceedings Appendix.

35. A computing platform comprising:

a secure key-handling unit arranged to store a storage root key that forms the root node of a tree-structured node hierarchy the non-leaf nodes of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes, and

insecure storage for storing the hierarchy nodes other than the root node;

the key-handling unit comprising:

a memory for storing a current decryption-root key;

a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key; and

a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

36. A computing platform according to claim 35, wherein the setting arrangement is arranged to permit the selected non-leaf node, and thereby the decryption-root key, to be changed only upon a predetermined set of at least one condition being met.

37. A computing platform according to claim 36, wherein at least one predetermined condition comprises the receipt by the

key handling unit of an authorization value indicative of particular digital data.

38. A computing platform according to claim 37, wherein said authorization value is a digest of a protected process associated with the node that is intended to be the new selected non-leaf node.

39. A computing platform according to claim 36, wherein at least one predetermined condition comprises that a protected process associated with the node that is intended to be the new selected non-leaf node is about to be run by the computing platform.

40. A computing platform according to claim 39, wherein at least one predetermined condition comprises that any other currently-activated processes running on the computing platform are benign.

41. A computing platform according to claim 36, wherein at least one predetermined condition comprises that the key-handling apparatus is requested to change the selected non-leaf node by a root of trust of the computing platform.

42. A computing platform according to claim 35, wherein upon start up of the computing platform, the node at the head of the hierarchy, forms said selected non-leaf node.

44. A computing platform according to claim 35, wherein the key-handling unit is arranged always to hold securely the node at the head of the hierarchy, in unencrypted form.

46. A computing platform according to claim 35, wherein the key-handling unit is arranged to indicate the selected non-leaf node by signing a value associated with the node using an identity key associated with the key-handling unit.

47. A computing platform according to claim 35, wherein the key-handling unit is so arranged that only a particular type of non-leaf node, herein a dynamic key node, can be used as the selected non-leaf node in addition to the node at the head of the hierarchy.

48. A computing platform according to claim 47, wherein the key-handling unit is arranged, upon receipt of a corresponding command, to generate a dynamic key node as a node of said hierarchy.

49. A computing platform according to claim 35, wherein the setting arrangement is arranged to permit the selected non-leaf node to be changed to one associated with a protected process upon receipt by the key-handling unit of a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes, the key of the non-leaf node associated with said protected process being available for use in relation to the protected process upon becoming the decryption root key.

No evidence is being submitted

No copies of decisions rendered in related proceedings are being submitted.